Orderly Generation of Half-Regular Symmetric Designs via Rahilly Families of Pre-Difference Sets

Priscila P. Alejandro, Anton Betten and Alice C. Niemeyer

Abstract

Rahilly families of pre-difference sets have been introduced by Rahilly, Praeger, Street and Bryant as a tool for constructing symmetric designs. Using orderly generation, we construct Rahilly families for various groups up to equivalence. For each equivalence class we determine the isomorphism type of the corresponding design. Some designs may be new, whilst others were already known in which case we identify them. For each design we test whether it admits as an automorphism group a regular extension of one of the given groups. If this is the case, the pre-difference set for the given group is also a difference set for the regular extension. We prove that there are examples of designs with a Rahilly family of pre-difference sets for a group which do not admit a regular extension.

Keywords: Rahilly family, symmetric design, orderly generation, difference set, half-regular automorphism group.

AMS subject classification: 05B05, 05B10, 51E05.

1 Introduction

Difference sets in groups can be used to construct symmetric designs admitting a regular group of automorphisms (cf. [1, VI. Theorem 1.6]). We say a group G acts *half-regularly* on a set Ω if it is semi-regular on Ω with exactly two orbits. We call a symmetric design *half-regular* if the design admits a group of automorphisms acting half-regularly on the point set. It is well known that such a half-regular group of automorphisms also acts half-regularly on the blocks.

Rahilly, Praeger, Street and Bryant [10] introduce a method for constructing half-regular symmetric designs. They define Rahilly families of pre-difference sets within groups. These

families generalize the concept of a difference set in a group. We present a brief summary of Rahilly families in Section 2. By construction, a Rahilly family for a group G gives rise to a symmetric design admitting G as a subgroup of its automorphism group acting half-regularly. Rahilly families can thus be used to obtain certain symmetric designs.

In this article, we describe a computer search to construct Rahilly families for small groups. Starting out with a putative parameter set we choose a group G of feasible order acting regularly on itself. Using the technique of orderly generation, we compute Rahilly families for such a group. We describe the method of orderly generation in Section 4, and in Section 5 we apply this strategy to construct Rahilly families as subsets of the given group. In addition, we consider Rahilly families up to equivalence, as introduced in [10]. As Rahilly families in the same class lead to isomorphic designs, we are only interested in finding one representative for each equivalence class. The equivalence classes can be described as orbits of a larger group on the set of all Rahilly families. Our algorithm is able to construct one particular representative of each class, which is called the canonical representative. It is the lexicographically least Rahilly set in its equivalence class. Moreover, we determine the group of auto-equivalences, that is the group of equivalences of the Rahilly family with itself. This group plays an important role in further investigations of properties of the corresponding symmetric design.

In Section 6 we present our results. We construct Rahilly families for groups of order 18 and 20 leading to 2-$(36, 15, 6)$ and 2-$(40, 13, 4)$ designs. In addition to the equivalence classes of Rahilly families we determine the isomorphism types of the corresponding designs. Further properties, including the action of the (full) automorphism groups, are also presented. Whenever possible, we identify previously known symmetric designs. We find half-regular symmetric designs which do not admit a regular group of automorphisms. This proves in particular that the set of designs which can be obtained from Rahilly families of pre-difference sets is larger than the set of designs obtainable from difference sets (Theorem 6.1).

2 Symmetric Designs from Rahilly Families

In this section we recall the basic definitions from [10] and summarize the results which are important for our purpose.

2.1 Rahilly Families

Let $\mathcal{D} = (\mathcal{V}, \mathcal{B})$ be a symmetric design with parameters 2-(v, k, λ). Thus the point-set $\mathcal{V} = \{p_1, p_2, \ldots, p_v\}$ has cardinality v and the block set $\mathcal{B}$ consists of v blocks, $B_1, \ldots, B_v$, say. Each block consists of k elements of $\mathcal{V}$ and every pair of points is contained in exactly λ blocks. The design can be described by a 0/1-*incidence-matrix*. This is a $v \times v$ matrix whose (i, j)-th entry is 1 if p_i is contained in B_j and 0 otherwise.

Any relabelling of the points results in a permutation of the rows of this matrix (and any reordering of the blocks corresponds to a permutation of its columns). The automorphism group, $\mathrm{Aut}(\mathcal{D})$, of this design consists of those permutations of the points which preserve the incidence matrix up to a reordering of its columns.

Assume that $\mathcal{D}$ admits a regular group G of automorphisms. Then any block $B \in \mathcal{B}$ can be chosen as a *base block* in the sense that any other block is the image of B under an element of G. A (v,k,λ)-*difference set* Δ for a group G of order v is a k-element subset of G such that each $g \in G\backslash\{1\}$ can be expressed exactly λ times as cd^{-1} with $c,d \in \Delta$. It can be shown that the blocks of a symmetric 2-(v,k,λ) design with regular group G of automorphisms are exactly the (v,k,λ)-difference sets for G. On the other hand, each (v,k,λ)-difference set Δ for a group G gives rise to a symmetric 2-(v,k,λ) design admitting G as a regular group of automorphisms. The blocks of this design are obtained from Δ by putting $B_1 := \Delta^{g_1}$, $B_2 := \Delta^{g_2}$, etc. where $g_1, g_2, \ldots$ runs through the elements of G.

Rahilly, Praeger, Street and Bryant in [10] consider half-regular symmetric designs $\mathcal{D}$ admitting a half-regular group G of automorphisms with orbits $\mathcal{V}_1$ and $\mathcal{V}_2$ on the point set $\mathcal{V}$. As mentioned above, G acts half-regularly on blocks, with block orbits $\mathcal{B}_1$ and $\mathcal{B}_2$. Half-regularity enforces $|\mathcal{V}_1| = |\mathcal{V}_2| = |\mathcal{B}_1| = |\mathcal{B}_2| = |G| = \frac{v}{2}$. Choose a point $p_i \in \mathcal{V}_i$, for $i = 1,2$, and call p_i the *base point* of $\mathcal{V}_i$. Any other point of $\mathcal{V}_i$ is the image of p_i under some element of G. As G acts regularly on both, $\mathcal{V}_1$ and $\mathcal{V}_2$, we can identify $\mathcal{V}_i$ with the set $\{g \times \{i\} \mid g \in G\}$, for $i = 1,2$.

Choose blocks $B_1 \in \mathcal{B}_1$ and $B_2 \in \mathcal{B}_2$. Define four subsets Δ_{ij} for $i,j \in \{1,2\}$ of G such that

$$\mathcal{V}_i \cap B_j = \Delta_{ij} \times \{i\}. \tag{2.1}$$

Then $k_{ij} = |\Delta_{ij}|$ for $i,j \in \{1,2\}$. Moreover, $k_{11} + k_{21} = k_{12} + k_{22} = k$ and $k_{11} = k_{22}$ and $k_{12} = k_{21}$ (see [10, Proposition 3.1]). These four sets are examples of what Rahilly et al. [10, Definition 2.1] call a Rahilly family of pre-difference sets:

Definition 2.1 *Let v,k,λ be positive integers with $k < v$ and v even. Let G be a finite group of order $\frac{v}{2}$ and let Δ_{ij} for $i,j \in \{1,2\}$ be a subset of G of size k_{ij} such that $k_{1j}+k_{2j} = k$. Then $\Delta = \{\Delta_{ij} \mid i,j \in \{1,2\}\}$ is called a* Rahilly family of pre-difference sets *for G with parameters (v,k,λ) if*

(a) for each $g \in G\backslash\{1\}$ and $i \in \{1,2\}$ there is an integer $\lambda_i(g)$ such that $0 \le \lambda_i(g) \le \lambda$ and g can be written exactly $\lambda_i(g)$ times as cd^{-1} with $c,d \in \Delta_{ii}$ and exactly $\lambda - \lambda_i(g)$ times as ef^{-1} with $e,f \in \Delta_{ij}$, where $\{i,j\} = \{1,2\}$;

(b) for each $g \in G$ and $\{i,j\} = \{1,2\}$ there is an integer $\lambda_i(g)$ such that $0 \le \lambda_{ij}(g) \le \lambda$ and g can be written exactly $\lambda_{ij}(g)$ times as cd^{-1} with $c \in \Delta_{ii}$ and $d \in \Delta_{ji}$ and exactly $\lambda - \lambda_{ij}(g)$ times as ef^{-1} with $e \in \Delta_{ij}$ and $f \in \Delta_{jj}$.

Rahilly families are useful for constructing half-regular symmetric designs: Given a Rahilly family Δ of pre-difference sets for a finite group G of order $\frac{v}{2}$ we obtain a symmetric 2-(v,k,λ) design $\mathcal{D} = (\mathcal{V},\mathcal{B})$ by putting $\mathcal{V} := G \times \{1,2\}$ and defining

$$B_i = \{(g,1) \mid g \in \Delta_{1i}\} \cup \{(g,2) \mid g \in \Delta_{2i}\}$$

for $i = 1,2$. Then G acts half-regularly on $\mathcal{V}$ via $(x,i)^g := (xg,i)$ for all $(x,i) \in \mathcal{V}$ and $g \in G$, (see [10, Proposition 2.3]). This action yields two orbits on blocks, namely $\mathcal{B}_1 = B_1^G$ and

$\mathcal{B}_2 = B_2^G$. We put $\mathcal{B} := \mathcal{B}_1 \cup \mathcal{B}_2$ and denote the design constructed in this way by $\mathcal{D}(\Delta)$. It is a half-regular symmetric design by [10]. As mentioned before, half-regular designs give rise to Rahilly families of pre-difference sets via Equation (2.1). If Δ is a Rahilly family of pre-difference sets obtained from a half-regular symmetric design $\mathcal{D}$ in this way then the symmetric design $\mathcal{D}(\Delta)$ is equal to $\mathcal{D}$ (see [10]).

2.2 Regular Extensions

Let $\mathcal{D}$ be a half-regular symmetric 2-(v, k, λ) design admitting a half-regular group G of automorphisms with Rahilly family of pre-difference sets $\Delta = \{\Delta_{11}, \Delta_{12}, \Delta_{21}, \Delta_{22}\}$. A group R of automorphisms of $\mathcal{D}$ with $G \leq R$ and which is regular on $\mathcal{V}$ is called a *regular extension* of G. It can be shown (see [10, Proposition 7.3]) that if such a group exists then there is an element $\tau \in R$ such that $\Delta_{11} \cup \tau\Delta_{21}$ is a difference set for R (in the usual sense).

Now let Δ and $\tilde{\Delta}$ be Rahilly families of pre-difference sets in a group G and let $\mathcal{D}(\Delta) = (\mathcal{V}, \mathcal{B})$ and $\mathcal{D}(\tilde{\Delta}) = (\tilde{\mathcal{V}}, \tilde{\mathcal{B}})$ denote the corresponding symmetric designs with parameters (v, k, λ). As G acts half-regularly on $\mathcal{V}$ and $\tilde{\mathcal{V}}$, we can identify both with $G \times \{1, 2\}$. In [10], the authors investigate isomorphisms between $\mathcal{D}(\Delta)$ and $\mathcal{D}(\tilde{\Delta})$.

We begin by quoting some definitions and results from [10]. An element $\pi \in \mathrm{Sym}_{\mathcal{V}}$ fixing $G \times \{i\}$ setwise for $i \in \{1, 2\}$ induces two bijections from G onto itself, namely the maps π_i, where $(g^{\pi_i}, i) = (g, i)^{\pi}$ for all $g \in G$. The permutation π induces an isomorphism from $\mathcal{D}(\Delta)$ to another symmetric design. It is said to *induce an automorphism* of G if for some $\varphi \in \mathrm{Aut}(G)$

$$g^{\pi_i} = a_i \cdot g^{\varphi}$$

holds for all $g \in G$ and $i = 1, 2$.

Definition 2.2 *An isomorphism π from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$ for which there exists $\varphi \in \mathrm{Aut}(G)$ and elements $(a_1, a_2, c_1, c_2) \in G^4$ such that*

$$\pi : (g, i) \mapsto (a_i \cdot g^{\varphi}, i) \quad \text{and} \quad a_i \cdot \Delta_{ij}^{\varphi} = \tilde{\Delta}_{ij} \cdot c_j$$

for all $i, j \in \{1, 2\}$ is called an equivalence *between $\mathcal{D}(\Delta)$ and $\mathcal{D}(\tilde{\Delta})$ with* associated automorphism *φ and* associated translations *(a_1, a_2, c_1, c_2).*

The following theorem [10, Theorem 5.1] shows that equivalent designs are isomorphic and states a criterion when a permutation in $\mathrm{Sym}_{\mathcal{V}}$ induces an isomorphism between designs.

Theorem 2.3 *Let Δ and $\tilde{\Delta}$ be two Rahilly families of pre-difference sets in a group G with parameters (v, k, λ). Let $\mathcal{D}(\Delta)$ and $\mathcal{D}(\tilde{\Delta})$ denote the corresponding symmetric 2-(v, k, λ) designs with block orbits $\mathcal{B}_1$, $\mathcal{B}_2$ and $\tilde{\mathcal{B}}_1$, $\tilde{\mathcal{B}}_2$, respectively. Suppose that the permutation π of $G \times \{1, 2\}$ fixes $G \times \{i\}$ setwise for $i \in \{1, 2\}$. Then π induces an automorphism of G, and an isomorphism from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\tilde{\Delta})$ which maps $\mathcal{B}_1$ to $\tilde{\mathcal{B}}_1$ and $\mathcal{B}_2$ to $\tilde{\mathcal{B}}_2$ if and only if π is an equivalence.*

A corollary of this theorem [10, Corollary 5.5] shows that if π is an equivalence then π fixes the base point p_i if and only if $a_i = 1$. Let $E(G)$ denote the subgroup of $N_{\mathrm{Aut}\mathcal{D}}(G)$ fixing $\mathcal{V}_1$ and $\mathcal{V}_2$ setwise. Clearly, the set of all equivalences is a subgroup of $E(G)$ of index 1 or 2. It was shown in [10] that these two groups are in fact equal.

We are interested in constructing symmetric designs defined by a Rahilly family of pre-difference sets admitting a half-regular group of automorphisms G. When searching for designs with a given set of parameters one is generally interested in finding these designs up to isomorphism. In our case however we construct half-regular symmetric designs up to equivalence as their equivalence classes can be used to determine whether or not these designs have regular extensions.

The *conjugate Rahilly family of pre-difference sets for* G is the family $\bar{\Delta}$ defined by $\bar{\Delta}_{11} = \Delta_{22}$, $\bar{\Delta}_{12} = \Delta_{21}$, $\bar{\Delta}_{21} = \Delta_{12}$, $\bar{\Delta}_{22} = \Delta_{11}$. The design $\mathcal{D}(\bar{\Delta})$ is called the *conjugate design* of $\mathcal{D}(\Delta)$. The designs $\mathcal{D}(\Delta)$ and $\mathcal{D}(\bar{\Delta})$ are clearly isomorphic, as we are only rearranging points and blocks. By [10, Theorem 6.5], they are equivalent if and only if $N_{\mathrm{Aut}\mathcal{D}}(G)$ is transitive on $\mathcal{V}$.

For a group G, the equivalences of a half-regular symmetric design with itself are called *auto-equivalences*. Theorem 6.4 of [10] shows that the group of auto-equivalences coincides with $E(G)$.

The existence of regular extensions for $\mathcal{D}(\Delta)$ is related to the existence of certain equivalences between $\mathcal{D}(\Delta)$ and $\mathcal{D}(\bar{\Delta})$.

Theorem 2.4 [10, Theorem 7.1] *Let $\mathcal{D}(\Delta)$ be a symmetric design with half-regular group G and Rahilly family Δ of pre-difference sets. Then G has a regular extension if and only if there exists an equivalence π from $\mathcal{D}(\Delta)$ to $\mathcal{D}(\bar{\Delta})$ with associated automorphism $\theta \in \mathrm{Aut}(G)$ and associated translations $(1, z, u^{-1}, u^{\theta^{-1}} \cdot z)$ such that $z^\theta = z$ and θ^2 is the inner automorphism of G induced by z.*

3 Computing Rahilly Families I

Assume that 2-(v, k, λ) is a valid parameter set for a symmetric design with $\frac{v}{2}$, k_{11}, k_{12}, k_{21}, k_{22}, λ satisfying the numerical conditions of Section 2 for a Rahilly family (with $k_{11}+k_{21} = k$). We want to compute all possible Rahilly families for these parameters using a given group G of order $\frac{v}{2}$. We fix a labelling of group elements $g_1, g_2, \ldots, g_{\frac{v}{2}}$ and let $\bar{G}$ denote the left-regular representation of G on itself.

Our aim is to list all subsets

$$\Delta_{ij} \in \binom{G}{k_{ij}},$$

for $1 \leq i, j \leq 2$, satisfying the requirements of Definition 2.1. These sets are constructed via a backtrack-search using the methods described in this and in the following section. We apply a four-fold backtrack search, starting with constructing all possible Δ_{11}. For each

possible Δ_{11} all admissible Δ_{12} are computed, and these in turn are extended to admissible Δ_{21} and finally the search tries to complete the Rahilly family by listing all possible Δ_{22}.

The computation of the four subsets has to be done with respect to the action of the group of equivalences $E(G)$. It turns out that we can reduce this problem to the task of determining orbits of a group on subsets, which we call the subset orbit problem. We discuss this problem in the next section. In Section 5, we return to Rahilly families and describe how we can apply the techniques of the subset orbit problem to the computation of equivalence classes of Rahilly families.

4 The Subset Orbit Problem

We consider a group G acting on a set $\mathcal{V} = \{p_1, \ldots, p_v\}$. Assume that there is another action of G on a possibly larger set X induced by the action of G on $\mathcal{V}$. We might, for example, consider the action of G on the set of subsets of $\mathcal{V}$, i.e. we take $X := \mathfrak{P}(\mathcal{V})$. Another example is the action of G on k-subsets for some $k \leq v$. Here, $X := \binom{\mathcal{V}}{k}$. For the remainder of this section, we consider the general situation of a group G acting on a set X. We call X a G-set.

The action of G imposes an equivalence relation on X by $x \sim_G y \iff \exists g \in G : x^g = y$ for $x, y \in X$. The equivalence classes of this relation are the orbits of G and the orbit of $x \in X$ is denoted by x^G. For $x \in X$, the stabilizer of x in G is the subgroup $G_x = \{g \in G \mid x^g = x\}$. For $g \in G$, the set of points fixed by g is $X_g = \{x \in X \mid x^g = x\}$. The set of orbits of G on X is denoted by $X//G$. A transversal is usually written as $\mathcal{T} = \mathcal{T}(X//G)$ indicating that $\mathcal{T}$ contains exactly one element of every G-orbit. For $A \subseteq X$, the pointwise stabilizer of A is $G_A = \{g \in G \mid a^g = a \text{ for all } a \in A\}$ and the setwise stabilizer of A is $G_{\{A\}} = \{g \in G \mid a^g \in A \text{ for all } a \in A\}$.

A fundamental problem is to determine the orbits of a group, for example by computing a transversal. If G acts on $\mathcal{V}$ and $X := \mathfrak{P}(\mathcal{V})$ or $X := \binom{\mathcal{V}}{k}$ for some $k \leq v$, we speak of the subset orbit problem. We shall discuss this problem in some detail here.

In the remainder of this section we discuss two important concepts which affect the efficiency of the algorithm we use for searching for Rahilly families.

Firstly, in Section 4.1 we introduce a lexicographical ordering on X. This allows us to define a canonical form for the orbit representatives of G on X as the lexicographically least element of the orbit. In Section 4.2 we present the algorithm "Orderly Generation" which solves the subset orbit problem by determining a transversal consisting of canonical elements. Originally, orderly generation has been invented as a tool for constructing graphs. Propably the first references are the articles of Read [11] and Colbourn and Read [3]. Canonical forms of graphs are discussed by McKay in [8].

If the action of G on $\mathcal{V}$ is intransitive, we can improve on this strategy even further by employing the concept of a G-morphism. This is a surjective mapping of the set X (the k-subsets of $\mathcal{V}$, for example) to another G-set Y which is in some sense compatible with the action. We discuss this idea in Section 4.3 and apply it to the computation of Rahilly families in Section 5.2. The morphism principle has been used by Laue for the construction

of soluble groups in [5].

4.1 Canonical Forms

Let us begin by recalling the concept of lexicographical order: We assume that $\mathcal{V} = \{p_1, p_2, \ldots, p_v\}$ is an ordered set, for instance by using the natural ordering $p_1 < p_2 < \ldots < p_v$. We say $A = \{a_1, \ldots, a_m\} \subseteq \mathcal{V}$ is *lexicographically less than* $B = \{b_1, \ldots, b_n\} \subseteq \mathcal{V}$ if there exists an index $\ell \in \{1, \ldots, \min\{m, n\}\}$ such that $a_1 = b_1, \ldots, a_{\ell-1} = b_{\ell-1}$ and $a_\ell < b_\ell$ holds or if n is greater than m and $\{b_1, \ldots, b_m\} = A$. Consider, for example, the three-element set $\mathcal{V} = \{1, 2, 3\}$. The elements of the power set $\mathfrak{P}(\mathcal{V})$ in lexicographical order are

$$\emptyset < \{1\} < \{1,2\} < \{1,2,3\} < \{1,3\} < \{2\} < \{2,3\} < \{3\}.$$

Returning to the action of G on X induced by the action on $\mathcal{V}$, we may now assume that the set X itself is an ordered set.

Assume the finite group G acts on the ordered set X. The lexicographically least element of a group orbit is called the *canonical representative*. For any $x \in X$ we put

$$\varphi(x) := \min_{g \in G} x^g$$

and call φ the *canonization map*. The elements of the form $\varphi(x)$ are called *canonical*. The set of group elements g mapping x onto its canonical form is the *transporter set*:

$$\tau(x) = \{g \in G \mid x^g = \varphi(x)\}.$$

Every element of the transporter set is a *transporter*.

The following properties of canonization maps are obvious:

C1: $\varphi^2 = \varphi$,

C2: $x \sim_G \varphi(x)$ for all $x \in X$,

C3: $x \sim_G y \iff \varphi(x) = \varphi(y)$ for all $x, y \in X$,

C4: $\varphi(x) = x \iff x$ is canonical,

The transversal of $X/\!/G$ consisting only of canonical elements is called *canonical transversal*. This transversal is unique. We denote it by $\mathcal{T}_<(X/\!/G)$, where the subscript refers to the ordering used. We have

C5: $\mathcal{T}_<(X/\!/G) = \text{Image}\,\varphi = \{\varphi(x) \mid x \in X\}$.

Let x, y be elements of X. The following facts are valid for transporter elements:

T1: Assume $x \sim_G y$. Let $g \in \tau(x)$ and $h \in \tau(y)$ be transporters. Then $x^g = \varphi(x) = \varphi(y) = y^h$ and thus $x^{gh^{-1}} = y$.

T2: Let $g \in \tau(x)$, then $G_{\varphi(x)} = gG_xg^{-1}$.

T3: Let $g, h \in \tau(x)$, then $gh^{-1} \in G_x$. Thus the set $\tau(x)$ forms a right coset of G_x in G.

4.2 Orderly Generation

In this section, we consider the task of determining the canonical transversal $\mathcal{T}_<(X/\!/G)$. According to C5, we might evaluate the canonization map for all k-subsets of $\mathcal{V}$. Of course, this strategy is unsatisfactory as its cost in terms of evaluations of φ is worst possible. We now describe the orderly generation algorithm.

For simplicity, assume that $\mathcal{V} = \{1, 2, \ldots, v\}$. In order to establish a recursive algorithm, we put $\mathcal{T}_<^{(i)} := \mathcal{T}_<(\binom{\mathcal{V}}{i}/\!/G)$ and also compute all $\mathcal{T}_<^{(i)}$ for $i = 0, 1, \ldots, k$. For $A = \{a_1, a_2, \ldots, a_k\} \in \binom{\mathcal{V}}{k}$ with $a_j < a_{j+1}$ for all $j < k$ we put $A \downarrow i = \{a_1, a_2, \ldots, a_i\}$ for $i \leq k$. The following lemma proves to be useful.

Lemma 4.1 *Let G be a group acting on the ordered set $\mathcal{V}$. Let $A = \{a_1, \ldots, a_k\}$ be a canonical k-subset of $\mathcal{V}$. Then, for any $i \leq k$, the restricted set $A \downarrow i$ is canonical. In other words,*

$$A \in \mathcal{T}_<^{(k)} \;\Rightarrow\; A \downarrow i \in \mathcal{T}_<^{(i)} \;\text{ for all }\; i \leq k.$$

Proof: We may require the elements of A being ordered $a_1 < a_2 < \ldots < a_k$. Assume that $A \downarrow i$ is not canonical for some $i < k$. Then there exists an element $g \in G$ with

$$(A \downarrow i)^g = \{b_1, \ldots, b_i\} < \{a_1, \ldots, a_i\} = A \downarrow i$$

where we assume that $b_1 < b_2 < \ldots < b_i$. By definition of the lexicographical order there exists an $h \leq i$ such that $b_j = a_j$ for $j = 1, \ldots, h-1$ and $b_h < a_h$. We now show that $A^g = \{b_1, \ldots, b_i\} \cup \{a_{i+1}^g, \ldots, a_k^g\}$ is less that $A = \{a_1, \ldots, a_k\}$ contradicting the canonicity of A. Note that some of the a_j^g with $i+1 \leq j \leq k$ may be less than b_h. Suppose that this is the case and let l be minimal such that $a_l^g < b_h$. If $a_l^g < b_1$ then since $b_1 \leq a_1$ we have $A^g < A$. So suppose that $b_1 < a_l^g$. Let h' be maximal such that $b_{h'} < a_l^g$. By assumption $h' < h$, and we have $b_1 = a_1, \ldots, b_{h'} = a_{h'}$, and the next smallest element of A^g is a_l^g, which is less than $b_{h'+1}$, which in turn is less than or equal to $a_{h'+1}$. Hence again $A^g < A$. Thus we may assume that all of the a_j^g are greater than b_h, and hence $b_1, \ldots, b_h$ are the smallest h elements of A^g in order. In this final case also we see that $A^g < A$. □

We call a set B with $B \downarrow j = A$ an *extension* of the set A. From Lemma 4.1 we conclude that each canonical $(j+1)$-set can be obtained as an extension of a unique canonical j-set. So, in order to construct $\mathcal{T}_<^{(j+1)}$ from $\mathcal{T}_<^{(j)}$ we consider each set $A \in \mathcal{T}_<^{(j)}$ and construct all sets B of size $j+1$ with $B \downarrow j = A$. We may write $A = \{a_1, \ldots, a_j\}$ with $a_i < a_{i+1}$ for all $i = 0, \ldots, j-1$. Then, $B = \{a_1, \ldots, a_j, a_{j+1}\}$ with $a_{j+1} > a_j$ (for otherwise $B \downarrow j$ would not be A). The elements a_{j+1} which we have to consider for extensions are

$$\mathrm{Ext}(A) = \mathcal{V} \setminus \{1, 2, \ldots, a_j\} = \{a_j + 1, \ldots, v\}.$$

With these elements, we can form the *candidate sets*:

$$\mathrm{Cand}(A) := \{A \cup \{a\} \mid a \in \mathrm{Ext}(A)\}.$$

The canonical transversal of $(j+1)$-orbits can be obtained in the following way:

$$\mathcal{T}_<^{(j+1)} = \bigcup_{A \in \mathcal{T}_<^{(j)}} \{B \in \mathrm{Cand}(A) \mid B \text{ is canonical } \}.$$

Using this inductive construction of canonical sets we obtain a tree, the generation tree:

The *generation tree* for $\mathcal{T}_<(\binom{\mathcal{V}}{k}//G)$ has the canonical i-sets $\mathcal{T}_<^{(i)} = \mathcal{T}_<(\binom{\mathcal{V}}{i}//G)$ for $0 \le i \le k$ as its set of nodes. The elements of $\mathcal{T}_<^{(i)}$ form the nodes at depth i in this tree. $\mathcal{T}_<^{(0)} = \emptyset$ is the root and the sets of $\mathcal{T}_<^{(k)}$ correspond to leaves of this tree. A set B is called *descendant* of a set A if B is an extension of A, i.e. if $B \downarrow |A| = A$. In this case, A is called *ancestor* of the set B. An *immediate descendant* is a descendant B of A with $|B| = |A| + 1$ (in this case, A is called *immediate ancestor* of B). Two sets A and B are joined by an edge if and only if B is an immediate descendant of A. If B is an immediate descendant of A, the node B is labelled by the unique element of $B \setminus A$. The set associated with a node of the tree can be reconstructed by following the path from the root to the node and collecting all labels encountered along this path. Moreover, by the definition of extension sets the labels along this path are lexicographically increasing.

We arrive at the following general algorithm to construct representatives of group orbits. Let the group G act on the finite set $\mathcal{V} = \{1, \ldots, v\}$ and let k be a number less than or equal to $|\mathcal{V}| = v$. The output of the following recursive algorithm is the canonical transversal $\mathcal{T}_<^{(k)} = \mathcal{T}_<(\binom{\mathcal{V}}{k}//G)$. Initially, we put $\mathcal{T}_<^{(k)} := \emptyset$. The input consists of the group G, the set $\mathcal{V}$ and the integer k. The integer i determines the depth of the recursion and should be set to 1 for the first call. The i-th element of the set A is addressed as a_i.

```
Procedure CanonicalTransversal(G, V, k, A, i)
    // now A = {a_1, ..., a_{i-1}}
    if i = k then add A to T_<^(k);
    else
        compute E = Ext({a_1, ..., a_{i-1}});
        for each e ∈ E do
            a_i := a;
            if IsCanonical(A ∪ {a_i}, G) then
                // A is canonical with respect to the action of G
                CanonicalTransversal(G, V, k, A, i + 1);
            endif;
        end;
    endif;
end (of CanonicalTransversal)
```

A few comments are in order:

1. If $i = 1$, we put $\mathrm{Ext}(\{\}) := \mathcal{V}$, otherwise $\mathrm{Ext}(\{a_1, \ldots, a_{i-1}\}) := \{a_{i-1} + 1, \ldots, v\}$.

2. The function IsCanonical(A, G) checks whether the set A is canonical with respect to G. We call this a *test for canonicity*. It involves a backtrack search through the elements of G to test whether there is a $g \in G$ with $A^g < A$. If this search does not succeed, i.e. if there is no such element, the canonicity of A has been proven. One such backtrack algorithm, the partition backtrack algorithm, involves the use of partitions of the set $\mathcal{V}$. An exhaustive treatment of this topic has been given by Leon in [6] and [7]. Recently, partition backtracking has been used by Theißen for the computation of normalizers in permutation groups [12].

3. The complexity of the algorithm is determined by the most difficult step which is the canonicity test. In order to compute the running time in terms of the number of calls to IsCanonical we note the following: In the i-th step, we extend all sets belonging to $\mathcal{T}_<^{(i)}$. Each such set has $|\mathcal{V}| - \Delta[i]$ candidates. Thus, the work in the i-th step is bounded above by $O(|\mathcal{T}_<^{(i)}| \cdot |V|)$. A rough estimation for the overall complexity can be obtained by bounding all $|\mathcal{T}_<^{(i)}|$ by $|\mathcal{T}_<^{(k)}|$. This yields $O(|\mathcal{T}_<^{(k)}|^k \cdot v)$ for the overall running time of CanonicalTransversal in calls to the procedure IsCanonical (we may leave out the computation of $\mathcal{T}_<^{(0)}$ which is done in a constant amount of time). However, we will show below how to avoid much of this work.

The following lemma reduces the number of extensions for a given set $A \in \mathcal{T}_<^{(i)}$.

Lemma 4.2 *Let G act on the lexicographically ordered set $\mathcal{V}$. Let A be a canonical i-set with set-stabilizer $G_{\{A\}}$. For $a \in \mathcal{V} \setminus A$ we form the set $A \cup \{a\}$. Then this set is not canonical if a is not canonical under $G_{\{A\}}$. In other words:*

$$A \in \mathcal{T}_<(\binom{\mathcal{V}}{i}//G),\ a \notin \mathcal{T}_<((\mathcal{V} \setminus A)//G_{\{A\}}) \ \Rightarrow\ A \cup \{a\} \notin \mathcal{T}_<(\binom{\mathcal{V}}{i+1}//G).$$

Proof: Let $a \notin \mathcal{T}_<((\mathcal{V} \setminus A)//G_{\{A\}})$ and $s \in G_{\{A\}}$ with $a^s = b < a$. Then

$$(A \cup \{a\})^s = A^s \cup \{a\}^s = A \cup \{b\} < A \cup \{a\},$$

showing that $A \cup \{a\}$ is not canonical with respect to G. □

The previous lemma allows us to reduce the number of elements which have to be considered for possible extensions of the set A. We may thus switch over to reduced extension sets:

$$\mathrm{Ext}(A) = \mathcal{T}_<((\mathcal{V} \setminus A)//G_{\{A\}}) \cap \{\max A + 1, \ldots, v\}.$$

According to the previous lemma, the above algorithm for constructing orbit representatives still produces the correct result but with generally far fewer calls to IsCanonical.

4.3 Exploiting Morphisms of Group Actions

An important tool for constructing group orbits is the use of G-morphisms. In some situations, a given group action induces an action on a smaller set which is in some sense

compatible with the original action. The computation of orbits is often easier by first determining the orbits of the smaller action and then extending the solution to the set of orbits of the original action. More precisely, we employ the concept of a G-morphism for a finite action as introduced for example in Neumann et al. [9, Chapter 7]. Assume we have two finite G-sets X and Y and there is an surjective mapping $\eta : X \to Y$ which is *compatible* with the group action, that is,

$$(x^g)^\eta = (x^\eta)^g \text{ holds for all } g \in G, x \in X.$$

We call η a *G-morphism* and write

$$X \overset{\eta}{\twoheadrightarrow}_G Y.$$

We call the actions of G on X and Y *compatible*.

Example 4.3 *Let G be a group acting on the finite set $\mathcal{V}$. Let k be an integer less than or equal to $v = |\mathcal{V}|$. Assume that G acts intransitively on $\mathcal{V}$ with two orbits $\mathcal{V}_1$ and $\mathcal{V}_2$.*

1. *We want to compute the orbits of G on k-subsets of $\mathcal{V}$, so we consider the G set $X := \binom{\mathcal{V}}{k}$. Then, the map*

$$\eta : \binom{\mathcal{V}}{k} \to \mathfrak{P}(\mathcal{V}_1) : \ D \mapsto D \cap \mathcal{V}_1$$

   is compatible with the action of G. If we restrict the image to the set of subsets of $\mathcal{V}_1$ of size $\leq k$, the map η becomes surjective.

2. *Assume we want to compute only those k-subsets of $\mathcal{V}$ which intersect $\mathcal{V}_i$ in k_i points, for $i = 1, 2$, where k_1 and k_2 are fixed integers with $k_1 + k_2 = k$. Let $\binom{\mathcal{V}}{k_1, k_2}$ be the set of k-subsets of $\mathcal{V}$ with his property. The map*

$$\eta : \binom{\mathcal{V}}{k_1, k_2} \to \binom{\mathcal{V}_1}{k_1} : \ D \mapsto D \cap \mathcal{V}_1$$

   is compatible with the action of G.

We get the following result for the relationship between the G-orbits.

Lemma 4.4 *(Morphism principle of group actions) Let X and Y be G-sets which are compatible with respect to a surjective G-morphism η. Then:*

1. *Two elements x_1 and x_2 in X with $x_1^\eta = x_2^\eta = y \in Y$ lie in the same G-orbit if and only if they lie in the same orbit of the stabilizer G_y.*

2. *A transversal for the orbits $X//G$ is*

$$T := \bigcup_{y \in \mathcal{T}(Y//G)} \mathcal{T}(y^{\eta^{-1}} // G_y).$$

Proof:

1. Assume that there exists an element $g \in G$ with $x_1 = x_2^g$. The G-morphism η allows to write

$$y^g = (x_2^\eta)^g = (x_2^g)^\eta = x_1^\eta = y,$$

and from this we deduce that g belongs to the stabilizer G_y. The other direction of the proof is trivial.

2. Let x_1 be an arbitrary element of X. We must show that there are elements $x \in T$ and $g \in G$ with $x_1^g = x$. Put $y_1 := x_1^\eta$. Then there are elements $h \in G$ and $y \in \mathcal{T}(Y//G)$ with $y_1^h = y$. Thus

$$y_1^h = (y_1^{\eta^{-1}})^h = (y_1^h)^{\eta^{-1}} = y^{\eta^{-1}} = x_2.$$

By the definition of $\mathcal{T}(X//G)$, there are elements $x \in \mathcal{T}(y^{\eta^{-1}}//G_y) \subseteq T$ and $u \in G_y$ with $x_2^u = x$. Thus $x_1^{hu} = x \in T$.

In addition, we must prove that no two elements of T are in the same G-orbit. Assume that $x_1^g = x_2$ with $g \in G$ and $x_1, x_2 \in T$. Put $y_1 := x_1^\eta$ and $y_2 := x_2^\eta$. By the definition of T, both y_1 and y_2 belong to $\mathcal{T}(Y//G)$ and $x_1 \in \mathcal{T}(y_1^{\eta^{-1}}//G_{y_1})$ and $x_2 \in \mathcal{T}(y_2^{\eta^{-1}}//G_{y_2})$. But

$$y_1^g = (x_1^\eta)^g = (x_1^g)^\eta = x_2^\eta = y_2,$$

which is possible only if $y_1 = y_2 =: y$ as both belong to the transversal $\mathcal{T}(Y//G)$. Thus $g \in G_y$ and $x_1, x_2 \in \mathcal{T}(y^{\eta^{-1}}//G_y)$. But $x_1^g = x_2$ which again by the property of a transversal is possible only if $x_1 = x_2$. This completes the proof.

□

In the case that we are working with ordered sets $(X, \leq)$ and $(Y, \leq)$ we may require the surjective G morphism $\eta : X \to Y$ to be compatible with the ordering, i.e.

$$x_1 \leq x_2 \;\Rightarrow\; x_1^\eta \leq x_2^\eta \qquad \forall\, x_1, x_2 \in X.$$

We write $(X, \leq) \overset{\eta}{\twoheadrightarrow}_G (Y, \leq)$ and call these *compatible actions on ordered sets.* We get the following refined version of the morphism principle:

Lemma 4.5 *(morphism principle for group actions on ordered sets) Let $\eta : X \to Y$ be a surjective mapping compatible with the action of G on the ordered sets $(X, \leq)$ and $(Y, \leq)$. Then*

$$\mathcal{T}_<(X//G) = \bigcup_{y \in \mathcal{T}_<(Y//G)} \mathcal{T}_<(y^{\eta^{-1}}//G_y).$$

Proof: Let T denote the right hand side of the equation. We must show that all elements in T are in fact canonical. Assume there is an element $x_1 \in X$ with $x_1 = x^g \leq x$ for some $g \in G$ and some $x \in T$. Put $y := x^\eta$ and $y_1 := x_1^\eta$. Then, by definition $y_1 \leq y$ and $y_1^{g^{-1}} = (x_1^\eta)^{g^{-1}} = (x_1^{g^{-1}})^\eta = x^\eta = y$. As $\mathcal{T}_<(Y/\!/G)$ is the canonical transversal for Y it follows that $y_1 = y$ and $g \in G_y$. Thus, x and x_1 both belong to $y^{\eta^{-1}}$. Further, $x \in \mathcal{T}_<(y^{\eta^{-1}}/\!/G_y) \subseteq T$ yields $x_1 = x$. This shows that T is the canonical transversal for the set of orbits $X/\!/G$. □

5 Computing Rahilly Families II

In order to compute Rahilly families algorithmically, we reduce the problem to determining all possible Δ to the subset orbit problem. We consider Δ as a $2 \cdot k$-subset of a suitable larger set and apply the orderly generation algorithm of Section 4.2 to the computation of all possible subsets satisfying the requirements of a pre-difference set. In addition, we make use of the special structure of Rahilly sets. We begin by computing all possible sets Δ_{11} and then extend the result by adding all possible Δ_{12}, Δ_{21} and Δ_{22}. This strategy is based on the use of G-morphisms as described in Section 4.3. We define a chain of morphisms which are compatible with the group action and then work along this chain in the reverse direction. The Rahilly families then appear at the end of this chain, when the four tuple of sets Δ_{ij} is completed.

5.1 Reduction to the Set Orbit Problem

The next result allows to describe the equivalence classes of Rahilly families as orbits of a group on a particular set. This enables us to use Procedure CanonicalTransversal to compute a transversal.

We take four copies of the set G: For $1 \leq i \leq 4$, we put $\mathcal{W}_i = \{i\} \times G = \{\{i\} \times g \mid g \in G\}$. Note that we take $\{i\} \times g$ here as the elements of the form $g \times \{i\}$ have already been introduced. We declare $\mathcal{W}^{(i)} := \bigcup_{j=1}^{i} \mathcal{W}_i$ and for simplicity, we put $\mathcal{W} = \mathcal{W}^{(4)}$. Let $p(\{i\} \times g) := g$ be the projection onto the second coordinate. For $H \subseteq \mathcal{W}_i$ we put $p(H) := \{p(h) \mid h \in H\}$.

For $i \leq 4$, let $\binom{\mathcal{W}^{(i)}}{k_1, \ldots, k_i}$ denote the subsets of $\mathcal{W}^{(i)}$ intersecting $\mathcal{W}_j$ in k_j elements for $j \leq i$. For $2 \leq i \leq 4$, we have the natural restrictions

$$\eta_i : \binom{\mathcal{W}^{(i)}}{k_1, \ldots, k_i} \mapsto \binom{\mathcal{W}^{(i-1)}}{k_1, \ldots, k_{i-1}},\ A \mapsto A \cap \mathcal{W}^{(i-1)}. \tag{5.1}$$

Each Rahilly family $\Delta = (\Delta_{11}, \Delta_{12}, \Delta_{21}, \Delta_{22})$ embeds into $\binom{\mathcal{W}}{k_1, \ldots, k_4}$ in the following way:

$$\Delta \mapsto (\{1\} \times \Delta_{11}) \cup (\{2\} \times \Delta_{12}) \cup (\{3\} \times \Delta_{21}) \cup (\{4\} \times \Delta_{22}).$$

On the other hand, each subset $D \in \binom{\mathcal{W}}{k_1,\ldots,k_4}$ defines a four-fold sequence of subsets of group elements Δ_D via:

$$\binom{\mathcal{W}}{k_1,\ldots,k_4} \mapsto \mathfrak{P}(G)^4,\ D \mapsto \Delta_D\ :=\ (p(D\cap\mathcal{W}_1),\ p(D\cap\mathcal{W}_2),\ p(D\cap\mathcal{W}_3),\ p(D\cap\mathcal{W}_4)).$$

For $i \leq 4$, we call a set $D \in \binom{\mathcal{W}^{(i)}}{k_1,\ldots,k_i}$ *admissible* if Δ_D is a partial Rahilly family, that is, if Δ_D fulfils the conditions of Definition 2.1. Let $\mathcal{R}(\mathcal{W}^{(i)})$ be the admissible subsets contained in $\binom{\mathcal{W}^{(i)}}{k_1,\ldots,k_i}$ (the letter $\mathcal{R}$ should remind us that these sets come from Rahilly families).

Recall from Section 2 that two Rahilly families Δ and $\hat{\Delta}$ are equivalent if and only if there exists a 5-tuple $(\varphi, a_1, a_2, c_1, c_2) \in \mathrm{Aut}(G) \times G^4$ mapping one to the other according to Definition 2.2. Each element $(\varphi, a_1, a_2, c_1, c_2) \in \mathrm{Equiv}(G) := \mathrm{Aut}(G) \times G^4$ induces a permutation $\pi_{\varphi,a_1,a_2,c_1,c_2} \in \mathrm{Sym}_{\mathcal{W}}$ via the following definition:

$$\{i\} \times g \mapsto \begin{cases} \{1\} \times a_1 \cdot g^{\varphi} \cdot c_1^{-1} & \text{if } i = 1, \\ \{2\} \times a_1 \cdot g^{\varphi} \cdot c_2^{-1} & \text{if } i = 2, \\ \{3\} \times a_2 \cdot g^{\varphi} \cdot c_1^{-1} & \text{if } i = 3, \\ \{4\} \times a_2 \cdot g^{\varphi} \cdot c_2^{-1} & \text{if } i = 4. \end{cases}$$

We have a map $\theta : \mathrm{Equiv}(G) \to \mathrm{Sym}_{\mathcal{W}} : (\varphi, a_1, a_2, c_1, c_2) \mapsto \pi_{\varphi,a_1,a_2,c_1,c_2}$. Put $Q := \mathrm{Equiv}(G)^{\theta} \leq \mathrm{Sym}_{\mathcal{W}}$. This means that Q acts on the set $\mathcal{W}$ and therefore also on the set of subsets of $\mathcal{W}$. We remark the following:

Proposition 5.1 *1. The equivalence classes of Rahilly families are in one-to-one correspondence with the orbits of Q on $\mathcal{R}(\mathcal{W})$.*

2. *The restrictions η_i defined by (5.1) are compatible with the action of Q.*

3. *The kernel of the mapping θ consists of the elements of the group $\langle(\mathrm{inn}_g, g, g, g^{-1}, g^{-1}) \mid g \in G\rangle$ (with $\mathrm{inn}_g : G \to G : x \mapsto x^g$). Thus, the order of Q is $|\mathrm{Equiv}(G)|/|G| = |\mathrm{Aut}(G)| \cdot |G|^3$.*

This proposition shows that we can obtain a transversal for the equivalence classes of Rahilly families by computing the orbits of Q on $\mathcal{R}(\mathcal{W})$, that is $\mathcal{T}_<(\mathcal{R}(\mathcal{W})//Q)$ is the required transversal of Rahilly families.

However, the action of Q on $\mathcal{W}$ and thus also on $\mathcal{R}(\mathcal{W})$ is not transitive. Therefore the morphism problem allows us to divide this orbit problem into several smaller pieces. This is discussed in the next section.

5.2 Inductive Construction via G-Morphisms

We apply a version of the morphism principle for ordered sets (Lemma 4.5) to the construction of Rahilly families by using a suitable Q-morphism together with a chain of Q-sets.

Consider the chain sets $\mathcal{W}^{(1)} \subseteq \mathcal{W}^{(2)} \subseteq \mathcal{W}^{(3)} \subseteq \mathcal{W}^{(4)}$, giving us a natural embedding of $\binom{\mathcal{W}^{(i)}}{k_1,\ldots,k_i}$ into $\binom{\mathcal{W}^{(i+1)}}{k_1,\ldots,k_i,k_{i+1}}$ for $i = 1,2,3$. The group Q leaves the sets $\mathcal{W}_i$ invariant, and thus the restriction maps η_i are compatible with the action:

$$(D^\pi)^{\eta_i} = (D^{\eta_i})^\pi \quad \text{for } i = 2,3,4$$

and for all $D \in \binom{\mathcal{W}^{(i)}}{k_1,\ldots,k_i}$ and $\pi \in Q$. Thus the same is true for admissible subsets, i.e.

$$(D^\pi)^{\eta_i} = (D^{\eta_i})^\pi \quad \text{for } i = 2,3,4$$

and for all $D \in \mathcal{R}(\mathcal{W}^{(i)})$ and $\pi \in Q$.

Now we order the subsets of $\mathcal{W}$ by ordering the sequences

$$(p(\mathcal{W} \cap \mathcal{W}_1),\ p(\mathcal{W} \cap \mathcal{W}_2),\ p(\mathcal{W} \cap \mathcal{W}_3),\ p(\mathcal{W} \cap \mathcal{W}_4)) \tag{5.2}$$

lexicographically using the original ordering of subsets of G for the comparison of the four components. It is useful to note that the maps η_i are compatible with this ordering of subsets of $\mathcal{W}$ as they simply eliminate the least significant elements which are the rightmost elements of the sequences (5.2). Thus we have the following chain of surjective Q-morphisms between ordered Q-sets:

$$(\mathcal{R}(\mathcal{W}^{(4)}),\leq) \overset{\eta_4}{\twoheadrightarrow_Q} (\mathcal{R}(\mathcal{W}^{(3)}),\leq) \overset{\eta_3}{\twoheadrightarrow_Q} (\mathcal{R}(\mathcal{W}^{(2)}),\leq) \overset{\eta_2}{\twoheadrightarrow_Q} (\mathcal{R}(\mathcal{W}^{(1)}),\leq).$$

For $1 \leq i \leq 4$, let $\mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i)})//Q)$ be the transversal of Q-canonical admissible sets in $\mathcal{R}(\mathcal{W}^{(i)})$. According to Lemma 4.1, $\mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i)})//Q)^{\eta_i} \subseteq \mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i-1)})//Q)$. We construct these canonical transversals in an iterative manner using the morphism principle. Assume we have a transversal $\mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i)})//Q)$ for some $i < 4$. Then, for each canonical admissible set $D \in \mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i)})//Q)$ we also have computed the stabilizer $Q_{\{D\}}$. We form the preimage $D^{\eta_{i+1}^{-1}} \cap \mathcal{R}(\mathcal{W}^{(i+1)})$, that is, the set of admissible sets $\tilde{D} \in \mathcal{R}(\mathcal{W}^{(i+1)})$ mapping onto D under η_{i+1}. We determine a transversal of the $Q_{\{D\}}$-orbits on this set of extensions. The disjoint union of all these transversals gives the desired transversal:

$$\mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i+1)})//Q) = \bigcup_{D \in \mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(i)})//Q)} \mathcal{T}_<((D^{\eta_{i+1}^{-1}} \cap \mathcal{R}(\mathcal{W}^{(i+1)}))//Q_{\{D\}}).$$

As a result, we obtain the following algorithm for computing Rahilly families with respect to a group G:

Procedure AllRahillyFamilies(G, Q, k_{11}, k_{12}, k_{21}, k_{22})
    // compute $T_1 := \mathcal{T}_<(\mathcal{R}(\mathcal{W}^{(1)})//Q)$:

```
    T_1 := CanonicalTransversal(Q, W_1, k_11);
    for each D ∈ T_1 do
        // D corresponds to Δ_11
        // compute T_2 := T_<((D^{η_2^{-1}} ∩ R(W^(2)))//Q_{D}):
        T_2 := CanonicalTransversal(Q_{D}, W_2, k_12);
        for each D ∈ T_2 do
            // D corresponds to (Δ_11, Δ_12)
            // compute T_3 := T_<((D^{η_3^{-1}} ∩ R(W^(3)))//Q_{D}):
            T_3 := CanonicalTransversal(Q_{D}, W_3, k_21);
            for each D ∈ T_3 do
                // D corresponds to (Δ_11, Δ_12, Δ_21)
                // compute T_4 := T_<((D^{η_4^{-1}} ∩ R(W^(4)))//Q_{D}):
                T_4 := CanonicalTransversal(Q_{D}, W_4, k_22);
                for each D ∈ T_4 do
                    // D corresponds to (Δ_11, Δ_12, Δ_21, Δ_22)
                    print new equivalence class of Rahilly families: Δ_D
                end;
            end;
        end;
    end;
end (of AllRahillyFamilies)
```

6 Results

We begin by computing feasible parameters for Rahilly families of pre-difference sets in a manner described in [10, Section 4]. We show these putative parameter sets for groups of order $\frac{v}{2}$ with $v \leq 220$ in Table 1, where $\mathcal{G}_i$ denotes the set of groups of order i. We indicate the number of groups of order $\frac{v}{2}$ in the last column of the table. Apart from the alternating group A_5 of order 60, all groups are soluble. It has been pointed out in [10] that there is a Rahilly family for $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ with $v = 16$, $k_{11} = 4$ and $k_{12} = 2$. This family leads to the famous biplane 2-$(16, 6, 2)$.

6.1 Half-Regular 2-$(36, 15, 6)$ Designs

Our aim is to construct symmetric designs on 36 points with $k = 15$ and $\lambda = 6$. Therefore, we construct Rahilly families of pre-difference sets in the group $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ of order 18. The Rahilly family has block sizes $k_{11} = k_{22} = 9$, $k_{12} = k_{21} = 6$. We take the following presentation for G:

$$\{a, b, c \mid a^2 = 1,\, b^3 = 1,\, c^3 = 1,\, a^b = a,\, a^c = a,\, b^c = b\}.$$

Every group element has a unique expression of the form $g_i = a^{e_1} b^{e_2} c^{e_3}$ with nonnegative exponents satisfying $e_1 < 2$, $e_2 < 3$ and $e_3 < 3$. We number the group elements in the

$\frac{v}{2}$	k_{11}	k_{21}	λ	$\lvert\mathcal{G}_{\frac{x}{2}}\rvert$	$\frac{v}{2}$	k_{11}	k_{21}	λ	$\lvert\mathcal{G}_{\frac{x}{2}}\rvert$
8	4	2	2	5	60	20	15	10	13
18	9	6	6	5	72	36	30	30	50
20	8	5	4	5	77	11	7	2	1
28	7	4	2	4	78	18	13	6	6
32	16	12	12	51	80	30	24	18	52
33	15	11	10	1	88	28	22	14	12
35	14	10	8	1	98	49	42	42	5
39	13	9	6	2	102	17	12	4	4
48	12	8	4	52	104	26	20	10	14
50	25	20	20	5	105	42	35	28	2
56	21	16	12	13	110	40	33	24	6

Table 1: Feasible Parameter Sets of Half-Regular Symmetric Designs

following order:

$$\begin{array}{llllll} g_1 = 1 & g_4 = ab & g_7 = c & g_{10} = abc & g_{13} = c^2 & g_{16} = abc^2 \\ g_2 = a & g_5 = b^2 & g_8 = ac & g_{11} = b^2c & g_{14} = ac^2 & g_{17} = b^2c^2 \\ g_3 = b & g_6 = ab^2 & g_9 = bc & g_{12} = ab^2c & g_{15} = bc^2 & g_{18} = ab^2c^2 \end{array}$$

In the resulting regular permutation representation, the generators a, b and c correspond to

$$\begin{aligned} \rho_a &= (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18), \\ \rho_b &= (1,3,5)(2,4,6)(7,9,11)(8,10,12)(13,15,17)(14,16,18), \\ \rho_c &= (1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18). \end{aligned}$$

The automorphism group of G has order 48. Thus, the group Q is of order $|\mathrm{Aut}(G)| \cdot 18^3 = 279936$.

Using the algorithm AllRahillyFamilies, we compute all Rahilly families for this group. This means that we build the generation tree having the Q-canonical admissible subsets as its nodes. We found 16 Rahilly families of pre-difference sets. Remarkably, for all the Rahilly families, we found the same sets Δ_{11}, Δ_{12} and Δ_{21}, namely

$$\Delta_{11} = \{1,2,3,4,5,8,10,14,16\} \quad \text{and} \quad \Delta_{12} = \Delta_{21} = \{1,2,9,12,16,17\}.$$

We call the 16 equivalence classes $\mathcal{E}_i$, $i \in \{1,2,\ldots,16\}$. For each of these classes we display the set Δ_{22} in Table 2. The table indicates the order of the group of auto-equivalences $E(G)$, whether or not the Rahilly family is self conjugate and, in the case that it is not, the corresponding conjugate family. Among the 16 equivalence classes we found 11 different designs, denoted by $\mathcal{D}_1, \ldots, \mathcal{D}_{11}$ (different designs means pairwise non-isomorphic designs). The isomorphism type of the design $\mathcal{D}(\mathcal{E}_i)$ is listed in the last column.

The corresponding 11 designs are shown in Table 3. All designs turn out to be self-dual and self-polar. We determined the full automorphism group and its action on points, blocks

$\mathcal{E}_i$	Δ_{22}	$\lvert E(G)\rvert$	conjugate to	isomorphic to
1	$\{1,2,3,4,5,8,10,14,16\}$	2	itself	$\mathcal{D}_5$
2	$\{1,2,3,4,6,7,9,13,15\}$	2	itself	$\mathcal{D}_8$
3	$\{1,2,3,5,6,8,12,14,18\}$	4	itself	$\mathcal{D}_1$
4	$\{1,2,3,5,7,8,9,11,14\}$	1	itself	$\mathcal{D}_4$
5	$\{1,2,4,5,6,7,11,13,17\}$	4	itself	$\mathcal{D}_{11}$
6	$\{1,2,4,6,7,8,10,12,13\}$	1	itself	$\mathcal{D}_8$
7	$\{1,3,4,5,7,9,10,11,16\}$	2	$\mathcal{E}_{14}$	$\mathcal{D}_2$
8	$\{1,3,7,8,9,10,12,13,15\}$	1	itself	$\mathcal{D}_7$
9	$\{1,5,7,8,10,11,12,13,17\}$	2	itself	$\mathcal{D}_{10}$
10	$\{1,7,8,10,12,13,14,16,18\}$	2	$\mathcal{E}_{11}$	$\mathcal{D}_6$
11	$\{2,3,4,6,8,9,10,12,15\}$	2	$\mathcal{E}_{10}$	$\mathcal{D}_6$
12	$\{2,4,7,8,9,10,11,14,16\}$	1	itself	$\mathcal{D}_3$
13	$\{2,6,7,8,9,11,12,14,18\}$	2	itself	$\mathcal{D}_3$
14	$\{2,7,8,9,11,13,14,15,17\}$	2	$\mathcal{E}_7$	$\mathcal{D}_2$
15	$\{3,8,9,10,12,14,15,16,18\}$	4	itself	$\mathcal{D}_{11}$
16	$\{4,7,9,10,11,13,15,16,17\}$	4	itself	$\mathcal{D}_9$

Table 2: Equivalence Classes of Rahilly Families for $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

and flags. We list the orbit structure by showing the distribution of different orbit lengths together with the multiplicities. So, x^n, y^m indicates that there are n orbits of length x and m orbits of length y. The running time for computing these 16 equivalence classes was about 15 minutes on a Pentium Pro based machine with 200 MHz clock speed. The computation of the isomorphism types of designs took another 3 minutes.

Design $\mathcal{D}_1$ is isomorphic to a previously known design admitting the group $\mathbb{Z}_6 \times \mathbb{Z}_6$ as a regular group of automorphisms. Using the elements

$$\{\,11,\ 22,\ 33,\ 44,\ 55,\ 01,\ 02,\ 03,\ 04,\ 05,\ 10,\ 20,\ 30,\ 40,\ 50\}$$

as a starter block one arrives at the design by allowing independent cyclic shifts modulo 6 in both components.

Designs $\mathcal{D}_1, \mathcal{D}_{10}$ and $\mathcal{D}_{11}$ can be constructed from Latin squares of order 6:

1	2	3	4	5	6		1	3	2	4	5	6		1	2	3	4	5	6
2	1	5	6	3	4		3	2	1	5	6	4		2	1	6	5	4	3
4	6	1	3	2	5		2	1	3	6	4	5		3	5	1	6	2	4
3	5	4	1	6	2		6	5	4	1	2	3		4	6	5	1	3	2
6	4	2	5	1	3		4	6	5	3	1	2		6	4	2	3	1	5
5	3	6	2	4	1		5	4	6	2	3	1		5	3	4	2	6	1

Let the (i,j)-th entry of the Latin square be denoted by $L(i,j)$. In order to obtain a symmetric 2-$(36,15,6)$ design one labels the places of the square with numbers $1,\ldots,36$ (for example, the i,j-th place may get the number $(i-1)\cdot 6+j$). Then, for any place i_0, j_0

$\mathcal{D}_i$	$\lvert\mathrm{Aut}(\mathcal{D}_i)\rvert$	point-orbit structure	flag-orbit structure
1	432	36	$108, 216^2$
2	36	18^2	$18^6, 36^{12}$
3	72	36	$36, 72^7$
4	36	36	36^{15}
5	216	36	$36, 72, 108^4$
6	324	18^2	$54^4, 108^3$
7	324	36	108^5
8	648	36	$108^3, 216$
9	144	36	$36, 72^3, 144^2$
10	1944	36	$216, 324$
11	3888	36	$216, 324$

Table 3: Isomorphism Types of Half-Regular 2-$(36, 15, 6)$ Designs

$\mathcal{E}_i$	regular extension for
1 ($\mathcal{D}_5$)	$\theta = (a \mapsto a, b \mapsto b, c \mapsto c), z = 1, u = 1$
2 ($\mathcal{D}_8$)	$\theta = (a \mapsto a, b \mapsto b, c \mapsto c^2), z = 1, u = a$
3 ($\mathcal{D}_1$)	$\theta = (a \mapsto a, b \mapsto b^2, c \mapsto c^2), z = 1, u = 1$
5 ($\mathcal{D}_{11}$)	$\theta = (a \mapsto a, b \mapsto b^2, c \mapsto c), z = 1, u = a$
6 ($\mathcal{D}_8$)	$\theta = (a \mapsto a, b \mapsto c, c \mapsto b), z = 1, u = 1$

Table 4: Regular Extensions of the Rahilly Families for $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

we define a block of the design as

$$B_{\langle i_0, j_0\rangle} = (\{(i,j) \mid i = i_0\} \cup \{(i,j) \mid j = j_0\} \cup \{(i,j) \mid L(i,j) = L(i_0,j_0)\})\backslash\{(i_0,j_0)\}.$$

It is easy to see that the set of blocks $B_{\langle i_0,j_0\rangle}$ for $1 \le i_0, j_0 \le 6$ forms a design with the appropriate parameters (cf. [13], p. 198). Altogether, there are 12 Latin squares of order 6 (and 109 of them if one may not exchange rows with columns or columns with digits). The other Latin squares lead to 2-$(36, 15, 6)$ designs different from $\mathcal{D}_1, \ldots, \mathcal{D}_{11}$.

Finally, we would like to point out that $\mathcal{D}_{11}$ can also be obtained from a Spence difference set. See [4] for this construction.

For an exhaustive reference on symmetric designs one should consult the section by Tran van Trung in [2], pp. 75–87. Note that in this table, only one known design for each parameter case is listed. Thus there may be other designs among $\mathcal{D}_1, \ldots, \mathcal{D}_{11}$ which are known.

According to Theorem 2.4, the existence of a regular extension is equivalent to the existence of an equivalence with special properties. We found that exactly the Rahilly families $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3, \mathcal{E}_5$ and $\mathcal{E}_6$ possess such an equivalence with $\theta \in \mathrm{Aut}(G)$ and associated translations $(1, z, u^{-1}, u^{\theta^{-1}} \cdot z)$. Table 4 displays these equivalences. This means that the designs $\mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_6, \mathcal{D}_7, \mathcal{D}_9$ and $\mathcal{D}_{10}$ do not admit a regular extension for their corresponding Rahilly families (for the designs $\mathcal{D}_2$ and $\mathcal{D}_6$ this also follows by the fact that $\mathrm{Aut}(\mathcal{D}_2)$ and

$\mathrm{Aut}(\mathcal{D}_6)$ act intransitively on points, cf. Table 2). Remarkably, $\mathcal{E}_5$ has a regular extension but the family $\mathcal{E}_{15}$, also leading to the design $\mathcal{D}_{11}$, has none. This means that G is contained twice in $\mathrm{Aut}(\mathcal{D}_{11})$ acting as a half-regular group. In one case it has a regular extension and in the other case it has none.

We have proved the following result:

Theorem 6.1 *There are half-regular symmetric designs whose full automorphism group is not regular. In other words, the set of designs we can construct via Rahilly-families of difference sets is a proper superset of the set of designs constructible from difference sets.*

6.2 Half-Regular 2-$(40, 13, 4)$ Designs

Using the cyclic group of order 20, another previously known symmetric design was rediscovered. This design admits a cyclic group of automorphisms acting regularly. It is a 2-$(40, 13, 4)$ design which can be developed from the base block $\{1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35\}$ using cyclic shifts modulo 40 (see [2, pp. 75–87]). Clearly, the square of such an automorphism of order 40 consists of 2 cycles of length 20. This element generates the regular group of automorphisms acting half regularly on the design.

7 Acknowledgements

We thank Cheryl E. Praeger for many helpful discussions and suggestions. The first author acknowledges the support of the Engineering and Science Educational Project, Department of Science and Technology, Philippines. The second author thanks Professor Praeger for an invitation to Perth during December 1997 and January 1998. He also acknowledges the DFG grant Ke 201/17-1. The third author acknowledges the support of ARC large grant A69941071.

References

[1] Th. Beth, D. Jungnickel, and H. Lenz. *Design theory*, Cambridge University Press, Cambridge, 1986.

[2] C. J. Colbourn and J. H. Dinitz, editors. *The CRC handbook of combinatorial designs*, CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[3] C. J. Colbourn and R. C. Read, Orderly algorithms for graph generation, *Internat. J. Comput. Math.*, **7** (1979), 167–172.

[4] Y. J. Ionin, New Symmetric Designs from Regular Hadamard Matrices, *The Electronic Journal of Combinatorics* **5** (1998).

[5] R. LAUE. Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen. *Bayreuth. Math. Schr.*, **9** (1982).

[6] J. S. LEON, Permutation group algorithms based on partitions. I: Theory and algorithms. *J. Symb. Comput.* **12** (1991), 533–583.

[7] J. S. LEON, Partitions, refinements, and permutation group computation. In *Groups and computation II. Workshop on groups and computation, June 7–10, 1995, New Brunswick, NJ, USA.*, volume 28 of *DIMACS, Ser. Discrete Math. Theor. Comput. Sci.*, pages 123–158. American Mathematical Society., Providence, RI, 1997.

[8] B. D. MCKAY, Computing automorphisms and canonical labellings of graphs. In *Combinatorial mathematics (Proc. Internat. Conf. Combinatorial Theory, Australian Nat. Univ., Canberra, 1977)*, volume 686 of *Lecture Notes in Math.*, pages 223–232. Springer, Berlin, 1978.

[9] P. M. NEUMANN, G. A. STOY, and E. C. THOMPSON, *Groups and geometry*. Oxford Science Publications, Oxford: Oxford University Press, 1994.

[10] A. RAHILLY, C. E. PRAEGER, A. P. STREET, and D. E. BRYANT, Half-regular symmetric designs. *Australasian J. of Combinatorics*, **8** (1993), 1–26.

[11] R. C. READ, Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Math.*, **2** (1978), 107–120.

[12] H. THEISSEN, *Eine Methode zur Normalisatorberechnung in Permutationsgruppen mit Anwendungen in der Konstruktion primitiver Gruppen*. PhD thesis, Rheinisch-Westfälische Technische Hochschule, Aachen, 1997.

[13] J. H. VAN LINT and R. M. WILSON, *A course in Combinatorics*. Cambridge University Press, Cambridge, 1992.

Priscila P. Alejandro
Mathematics Department
University of the Philippines
Diliman QC 1101, Philippines
cristy@math01.cs.upd.edu.ph

Anton Betten
Fakultät für Mathematik und Physik
Universität Bayreuth
95440 Bayreuth, Germany
Anton.Betten@uni-bayreuth.de

Alice C. Niemeyer
Department of Mathematics,
University of Western Australia
Nedlands, WA 6907, Australia
alice@maths.uwa.edu.au